►B

SKLEP SVETA (SZVP) 2019/797

z dne 17. maja 2019

o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice

(UL L 129I, 17.5.2019, str. 13)

spremenjen z:

		Uradni list		
		št.	stran	datum
►M1	Sklep Sveta (SZVP) 2020/651 z dne 14. maja 2020	L 153	4	15.5.2020
►M2	Sklep Sveta (SZVP) 2020/1127 z dne 30. julija 2020	L 246	12	30.7.2020
►M3	Sklep Sveta (SZVP) 2020/1537 z dne 22. oktobra 2020	L 351 I	5	22.10.2020
►M4	Sklep Sveta (SZVP) 2020/1748 z dne 20. novembra 2020	L 393	19	23.11.2020
►M5	Sklep Sveta (SZVP) 2021/796 z dne 17. maja 2021	L 174 I	1	18.5.2021
►M6	Sklep Sveta (SZVP) 2022/754 z dne 16. maja 2022	L 138	16	17.5.2022

popravljena z:

►C1	Popravek, UL L 230, 17.7.2020, str. 36 (2019/797)	

▼B

SKLEP SVETA (SZVP) 2019/797

z dne 17. maja 2019

o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice

Člen 1

1. Ta sklep se uporablja za kibernetske napade s pomembnim učinkom in na poskuse kibernetskih napadov s potencialno pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam.

2. Med kibernetske napade, ki pomenijo zunanjo grožnjo, spadajo napadi:

(a) ki izvirajo ali so bili izvedeni iz držav zunaj Unije;

(b) pri katerih se uporablja infrastruktura zunaj Unije;

(c) ki jih je izvedla katera koli fizična ali pravna oseba, subjekt ali organ, ki ima sedež zunaj Unije ali ki deluje od tam ali

(d) ki so bili izvedeni s podporo, vodenjem ali pod nadzorom katere koli fizične ali pravne osebe, subjekta ali organa, ki deluje zunaj Unije.

3. V tem sklepu so kibernetski napadi dejanja, ki vključujejo kar koli od naslednjega:

(a) dostop do informacijskih sistemov;

(b) motnje informacijskega sistema;

(c) poseganje v podatke ali

(d) prestrezanje podatkov,

kadar teh dejanj ni ustrezno odobril lastnik ali drugi imetnik pravice do sistema ali podatkov oziroma do dela sistema ali podatkov ali ki jih ne dovoljuje pravo Unije ali zadevne države članice.

4. Med kibernetske napade, ki pomenijo grožnjo za državo članico, spadajo napadi z vplivom na informacijske sisteme, ki so med drugim povezani z naslednjim:

(a) ključno infrastrukturo, vključno s podvodnimi kabli in objekti, izstreljenimi v vesolje, ki je bistvena za ohranjanje ključnih funkcij v družbi ali zdravja, varnosti, zaščite, ekonomske ali socialne blaginje ljudi;

(b) storitvami, potrebnimi za ohranjanje bistvenih družbenih in/ali gospodarskih dejavnosti, zlati v sektorjih: energije (elektrika, nafta in plin); prevoza (zračni, železniški, vodni in cestni); bančništva;

▼B

infrastrukture finančnega trga; zdravstva (izvajalci zdravstvene dejavnosti, bolnišnice in zasebne klinike); oskrbe s pitno vodo in njeno distribucijo; digitalne infrastrukture; in v katerem koli drugem sektorju, bistvenem za zadevno državo članico;

(c) kritičnimi državnimi funkcijami, zlasti na področjih obrambe, vodenja in delovanja institucij, vključno z javnimi volitvami in postopki glasovanja volitev, delovanja gospodarske in civilne infrastrukture, notranje varnosti in zunanjih odnosov, vključno z diplomatskimi misijami;

(d) s shranjevanjem ali obdelavo tajnih podatkov ali

(e) vladnimi skupinami za ukrepanje v izrednih razmerah.

5. Med kibernetske napade, ki pomenijo grožnjo za Unijo, spadajo napadi, izvedeni proti njenim institucijam, organom, uradom in agencijam, njenim delegacijam v tretjih državah ali mednarodnih organizacijah, operacijam in misijam v okviru skupne vojaške in obrambne politike (SVOP) in njenim posebnim predstavnikom.

6. Kadar se to zdi potrebno za doseganje ciljev SZVP iz ustreznih določb člena 21 Pogodbe o Evropski uniji, se lahko omejevalni ukrepi iz tega sklepa uporabljajo tudi kot odziv na kibernetske napade, ki imajo znaten učinek na tretje države ali mednarodne organizacije.

Člen 2

V tem sklepu se uporabljajo naslednje opredelitve pojmov:

(a) „informacijski sistemi“ pomeni napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več v skladu s programom samodejno obdeluje digitalne podatke, kakor tudi digitalne podatke, ki so shranjeni, obdelani, pridobljeni ali se po tej napravi ali skupini naprav prenašajo zaradi njenega ali njihovega delovanja, uporabe, varovanja in vzdrževanja;

(b) „motnje informacijskega sistema“ pomeni oviranje ali prekinitev delovanja informacijskega sistema z vnašanjem digitalnih podatkov, prenašanjem, poškodovanjem, brisanjem, poslabšanjem, spreminjanjem ali odstranitvijo takih podatkov ali povzročitvijo nedostopnosti takšnih podatkov;

(c) „poseganje v podatke“ pomeni brisanje, poškodovanje, poslabšanje, spreminjanje ali odstranitev digitalnih podatkov v informacijskem sistemu ali povzročitev nedostopnosti takšnih podatkov; vključuje tudi krajo podatkov, sredstev, gospodarskih virov ali intelektualne lastnine;

(d) „prestrezanje podatkov“ pomeni prestrezanje nejavnega prenosa digitalnih podatkov v informacijski sistem, iz ali znotraj njega s tehničnimi sredstvi, vključno z elektromagnetnimi emisijami iz informacijskega sistema, ki prenašajo takšne digitalne podatke.

▼B

Člen 3

Dejavniki, ki odločajo o tem, ali ima kibernetski napad pomemben učinek iz člena 1(1), vključujejo kar koli od naslednjega:

(a) obseg, razsežnost, učinek ali resnost motnje, ki jih ta povzroči, vključno z gospodarskimi in družbenimi dejavnostmi, bistvenimi storitvami, kritičnimi državnimi funkcijami, javnim redom ali javno varnostjo;

(b) število prizadetih fizičnh ali pravnih oseb, subjektov ali organov;

(c) število zadevnih držav članic;

(d) znesek ekonomske izgube, povzročene na primer z obsežno krajo sredstev, gospodarskih virov ali intelektualne lastnine;

(e) gospodarska korist, ki jo pridobi storilec zase ali za druge;

(f) količina ali značaj ukradenih podatkov ali obseg kršitev varnosti podatkov ali

(g) značaj pridobljenih poslovno občutljivih podatkov.

Člen 4

1. Države članice sprejmejo potrebne ukrepe, da preprečijo vstop na svoja ozemlja ali tranzit preko njega:

(a) fizičnim osebam, ki so odgovorne za kibernetske napade ali poskuse kibernetskih napadov;

(b) fizičnim osebam, ki zagotavljajo finančno, tehnično ali materialno podporo ali so kako drugače vpletene v kibernetske napade ali poskuse kibernetskih napadov, na primer z njihovim načrtovanjem, pripravljanjem, sodelovanjem pri njih, njihovim vodenjem, pomočjo ali spodbujanjem takih napadov ali z njihovim omogočanjem bodisi z dejanji ali opustitvijo dejanj;

(c) fizičnim osebam, povezanim z osebami iz točk (a) in (b);

kot so navedene v Prilogi.

2. Odstavek 1 držav članic ne zavezuje k temu, da bi lastnim državljanom zavrnile vstop na svoje ozemlje.

3. Odstavek 1 ne posega v primere, v katerih posamezno državo članico zavezuje mednarodnopravna obveznost, in sicer:

(a) kot državo gostiteljico mednarodne medvladne organizacije;

(b) kot državo gostiteljico mednarodne konference, ki jo skliče OZN ali katere pokroviteljica je OZN;

(c) v skladu z večstranskim sporazumom o dodeljenih privilegijih in imunitetah, ali

(d) v okviru Lateranske pogodbe, ki sta jo leta 1929 sklenila Sveti sedež (Vatikanska mestna država) in Italija.

▼B

4. Za odstavek 3 se šteje, da se uporablja tudi, kadar je država članica gostiteljica Organizacije za varnost in sodelovanje v Evropi (OVSE).

5. Svet je ustrezno obveščen vsakič, ko posamezna država članica odobri izjemo v skladu z odstavkom 3 ali 4.

6. Države članice lahko odobrijo izjeme od ukrepov, uvedenih na podlagi odstavka 1, kadar je potovanje upravičeno zaradi nujnih humanitarnih potreb ali udeležbe na medvladnih srečanjih ali srečanjih, ki jih podpira ali gosti Unija ali ki jih gosti država članica, ki predseduje OVSE, in na katerih poteka politični dialog za neposredno spodbujanje uresničevanja ciljev politike omejevalnih ukrepov, vključno z varnostjo in stabilnostjo v kibernetskem prostoru.

7. Države članice lahko odobrijo izjeme od ukrepov, uvedenih na podlagi odstavka 1, kadar je vstop ali tranzit potreben zaradi izvedbe sodnega postopka.

8. Država članica, ki želi odobriti izvzetje iz odstavka 6 ali 7, o tem pisno uradno obvesti Svet. Izvzetje se šteje za odobreno, razen če eden ali več članov Sveta vloži pisni ugovor v dveh delovnih dneh po prejemu uradnega obvestila o predlaganem izvzetju. Če en ali več članov Sveta vloži ugovor, lahko Svet s kvalificirano večino odloči, da se predlagano izvzetje odobri.

9. Kadar država članica na podlagi odstavkov 3, 4, 6, 7 ali 8 osebam s seznama iz Priloge odobri vstop na svoje ozemlje ali tranzit preko njega, je odobritev strogo omejena na namen, za katerega je bila podeljena, in na osebe, na katere se neposredno nanaša.

Člen 5

1. Zamrznejo se vsa sredstva in gospodarski viri, ki pripadajo, so v lasti ali pod nadzorom:

(a) fizičnih ali pravnih oseb, subjektov ali organov, ki so odgovorni za kibernetske napade ali poskuse kibernetskih napadov;

(b) fizičnih ali pravnih oseb, subjektov ali organov, ki zagotavljajo finančno, tehnično ali materialno podporo ali so kako drugače vpletene v kibernetske napade ali poskuse kibernetskih napadov, na primer z njihovim načrtovanjem, pripravljanjem, sodelovanjem pri njih, njihovim vodenjem, pomočjo ali spodbujanjem takih napadov ali z njihovim omogočanjem bodisi z dejanji ali opustitvijo dejanj;

(c) fizičnih ali pravnih oseb, subjektov ali organov, ki so povezani s fizičnimi ali pravnimi osebami, subjekti ali organi iz točk (a) in (b),

kot so navedeni v Prilogi.

▼B

2. Fizičnim ali pravnim osebam, subjektom ali organom s seznama iz Priloge ne smejo biti neposredno ali posredno dana na razpolago ali v njihovo korist nikakršna sredstva ali gospodarski viri.

3. Z odstopanjem od odstavkov 1 in 2 lahko pristojni organi držav članic pod takšnimi pogoji, za katere menijo, da so primerni, odobrijo sprostitev določenih zamrznjenih sredstev ali gospodarskih virov ali razpolaganje z njimi, potem ko so ugotovili, da so sredstva ali gospodarski viri:

(a) ►C1 nujni za osnovne potrebe fizičnih in pravnih oseb, subjektov ali organov s seznama iz Priloge ◄ in vzdrževanih družinskih članov takih fizičnih oseb, vključno s plačili za živila, najemnine ali hipoteke, zdravila in zdravljenje, davke, zavarovalne premije in pristojbine za storitve javne komunale;

(b) namenjeni izključno za plačilo razumnih honorarjev ali nadomestil nastalih izdatkov, povezanih z zagotavljanjem pravnih storitev;

(c) namenjeni izključno za plačilo honorarjev ali stroškov storitev za redno hranjenje ali vzdrževanje zamrznjenih sredstev ali gospodarskih virov;

(d) potrebni za kritje izrednih izdatkov, če ustrezni pristojni organ vsaj dva tedna pred odobritvijo pristojnim organom drugih držav članic in Komisiji uradno sporoči razloge, na podlagi katerih meni, da je treba izdati posamezno odobritev, ali

(e) nakazani na račun ali z računa diplomatske ali konzularne misije ali mednarodne organizacije, ki ima imuniteto v skladu z mednarodnim pravom, če so taka plačila namenjena za uradne naloge diplomatske ali konzularne misije ali mednarodne organizacije.

Zadevna država članica obvesti druge države članice in Komisijo o vseh odobritvah, izdanih na podlagi tega odstavka.

4. Z odstopanjem od odstavka 1 lahko pristojni organi držav članic odobrijo sprostitev določenih zamrznjenih sredstev ali gospodarskih virov, če so izpolnjeni naslednji pogoji:

(a) sredstva ali gospodarski viri so predmet arbitražne odločbe, izdane pred datumom uvrstitve fizične ali pravne osebe, subjekta ali organa iz odstavka 1 na seznam iz Priloge, ali sodne ali upravne odločbe, izdane v Uniji, ali sodne odločbe, izvršljive v zadevni državi članici, pred navedenim datumom ali po njem;

▼B

(b) sredstva ali gospodarski viri se bodo uporabljali izključno za poravnavo terjatev, ki so zavarovane s tako odločbo ali so v taki odločbi priznane kot veljavne, v mejah, določenih z veljavno zakonodajo in predpisi, ki urejajo pravice oseb s takimi terjatvami;

(c) odločba ni v korist fizične ali pravne osebe, subjekta ali organa s seznama iz Priloge ter

(d) priznanje odločbe ni v nasprotju z javnim redom zadevne države članice.

Zadevna država članica obvesti druge države članice in Komisijo o vseh odobritvah, izdanih na podlagi tega odstavka.

5. Odstavek 1 fizični ali pravni osebi, subjektu ali organu s seznama iz Priloge ne preprečuje, da bi izvedel plačilo, zapadlo po pogodbi, ki je bila sklenjena pred datumom uvrstitve navedene fizične ali pravne osebe, subjekta ali organa na seznam v navedeni prilogi, pod pogojem, da je zadevna država članica ugotovila, da plačila neposredno ali posredno ne prejme fizična ali pravna oseba, subjekt ali organ iz odstavka 1.

6. Odstavek 2 se ne uporablja za prilive na zamrznjene račune, ki so:

(a) obresti ali drugi dohodki na navedenih računih;

(b) zapadla plačila po pogodbah, sporazumih ali obveznostih, sklenjenih ali nastalih pred datumom, ko so za te račune začeli veljati ukrepi iz odstavkov 1 in 2, ali

(c) zapadla plačila po sodnih, upravnih ali arbitražnih odločbah, izdanih v Uniji ali izvršljivih v zadevni državi članici,

pod pogojem, da za vse takšne obresti, druge dohodke in plačila še naprej veljajo ukrepi iz odstavka 1.

Člen 6

1. Svet na predlog države članice ali visokega predstavnika Unije za zunanje zadeve in varnostno politiko soglasno pripravi oziroma spremeni seznam iz Priloge.

2. Svet o sklepu iz odstavka 1, vključno z razlogi za uvrstitev na seznam, obvesti zadevno fizično ali pravno osebo, subjekt ali organ, bodisi neposredno, če je naslov znan, bodisi z objavo obvestila, s čimer da navedeni fizični ali pravni osebi, subjektu ali organu možnost, da predloži pripombe.

3. Kadar so predložene pripombe ali so predstavljeni novi tehtni dokazi, Svet pregleda sklep iz odstavka 1 in o tem ustrezno obvesti zadevno fizično ali pravno osebo, subjekt ali organ.

▼B

Člen 7

1. Priloga vključuje razloge za uvrstitev na seznam fizičnih in pravnih oseb, subjektov in organov iz členov 4 in 5.

2. Priloga vsebuje informacije, potrebne za identifikacijo zadevnih fizičnih ali pravnih oseb, subjektov ali organov, kadar so te informacije na voljo. Za fizične osebe lahko te informacije vključujejo: imena in vzdevke; datum in kraj rojstva; državljanstvo; številko potnega lista in osebne izkaznice; spol, naslov, če je znan; ter funkcijo ali poklic. Za pravne osebe, subjekte ali organe lahko te informacije vključujejo imena, kraj in datum registracije, matično številko in sedež podjetja.

Člen 8

V zvezi s kakršno koli pogodbo ali transakcijo, katere izvedba je bila neposredno ali posredno v celoti ali deloma ovirana zaradi ukrepov, uvedenih v skladu s tem sklepom, vključno z zahtevki za nadomestilo škode ali kakršnimi koli drugimi zahtevki te vrste, kot je odškodninski zahtevek ali zahtevek za uveljavljanje garancije, zlasti zahtevek za podaljšanje dospelosti ali za plačilo obveznice, garancije ali nadomestilo škode, zlasti finančne garancije ali finančnega jamstva v kakršni koli obliki, se ne ugodi nobenemu zahtevku, če ga vložijo:

(a) fizične ali pravne osebe, subjekti ali organi, uvrščeni na seznam iz Priloge,

(b) katera koli fizična ali pravna oseba, subjekt ali organ, ki deluje prek fizičnih ali pravnih oseb, subjektov ali organov iz točke (a) ali v njihovem imenu.

Člen 9

Da bi bili ukrepi, določeni v tem sklepu, čim bolj učinkoviti, Unija spodbuja tretje države k sprejetju omejevalnih ukrepov, podobnih tistim, ki so določeni v tem sklepu.

▼M6

Člen 10

Ta sklep se uporablja do 18. maja 2025 in se redno pregleduje. Ukrepi iz členov 4 in 5 se uporabljajo za fizične in pravne osebe, subjekte in organe s seznama v Prilogi do 18. maja 2023.

▼B

Člen 11

Ta sklep začne veljati na dan po objavi v *Uradnem listu Evropske unije*.

▼B

PRILOGA

Seznam fizičnih in pravih oseb, subjektov in organov iz členov 4 in 5

▼M2

A. Fizične osebe

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
▼M4				
1.	GAO Qiang	Datum rojstva: 4. oktober 1983 Kraj rojstva: Provinca Shandong, Kitajska Naslov: Soba 1102, Guanfu Mansion, ulica Xinkai 46, okrožje Hedong, Tjandžin, Kitajska Državljanstvo: kitajsko Spol: moški	Gao Qiang je vpleten v „Operation Cloud Hopper“, vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov, ki imajo pomemben učinek na tretje države. Tarča „Operation Cloud Hopper“ so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. „Operation Cloud Hopper“ je izvedel akter, v javnosti znan kot „APT10“ („Advanced Persistent Threat 10“) (tudi „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ in „Potassium“). Gao Qianga je mogoče povezati z APT10, med drugim zaradi njegove povezave z infrastrukturo APT10 za poveljevanje in kontrolo. Poleg tega je bil Gao Qiang zaposlen pri Huaying Haitai, ki je subjekt, uvrščen na seznam zaradi zagotavljanja podpore in omogočanja „Operation Cloud Hopper“. Povezan je z Zhang Shilongom, ki je prav tako uvrščen na seznam v povezavi z „Operation Cloud Hopper“. Gao Qiang je torej povezan s Huaying Haitai in Zhang Shilongom.	30.7.2020
2.	ZHANG Shilong	Datum rojstva: 10. september 1981 Kraj rojstva: Kitajska Naslov: Hedong, ulica Yuyang 121, Tjandžin, Kitajska Državljanstvo: kitajsko Spol: moški	Zhang Shilong je vpleten v „Operation Cloud Hopper“, vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov, ki imajo pomemben učinek na tretje države.	30.7.2020

▼M4

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
			Tarča „Operation Cloud Hopper“ so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. „Operation Cloud Hopper“ je izvedel akter, v javnosti znan kot „APT10“ („Advanced Persistent Threat 10“) (tudi „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ in „Potassium“). Zhang Shilonga je mogoče povezati z APT10, med drugim zaradi zlonamerne programske opreme, ki jo je razvil in testiral v povezavi s kibernetskimi napadi, ki jih je izvedel APT10. Poleg tega je bil Zhang Shilong zaposlen pri Huaying Haitai, ki je subjekt, uvrščen na seznam zaradi zagotavljanja podpore in omogočanja „Operation Cloud Hopper“. Povezan je z Gao Qiangom, ki je uvrščen na seznam v povezavi z „Operation Cloud Hopper“. Zhang Shilong je torej povezan s Huaying Haitai in Gao Qiangom.	

▼M2

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Datum rojstva: 27. maj 1972 Kraj rojstva: pokrajina Perm, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 120017582 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Alexej Minin je sodeloval pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot pomožni uradnik za HUMINT (zbiranje obveščevalnih podatkov z osebnimi stiki) v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020

▼M2

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Datum rojstva: 31. julij 1977 Kraj rojstva: pokrajina Murmansk, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 100135556 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Aleksei Morenets je sodeloval pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot kibernetski operater v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Datum rojstva: 26. julij 1981 Kraj rojstva: Kursk, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 100135555 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Evgenii Serebriakov je sodeloval pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot kibernetski operater v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020

▼M2

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Datum rojstva: 24. avgust 1972 Kraj rojstva: Uljanovsk, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 120018866 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Oleg Sotnikov je sodeloval pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot pomožni uradnik za HUMINT (zbiranje obveščevalnih podatkov z osebnimi stiki) v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020

▼M3

7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич Бадин Datum rojstva: 15. november 1990 Kraj rojstva: Kursk, Ruska SFSR (danes Ruska federacija) Državljanstvo: rusko Spol: moški	Dmitry Badin je sodeloval v kibernetskem napadu s pomembnim učinkom proti nemškemu zveznemu parlamentu (Deutscher Bundestag). Kot vojaški obveščevalni uradnik 85. glavnega centra za posebne storitve (GTsSS) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil Dmitry Badin član skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila in maja 2015 izvedla kibernetski napad na nemški zvezni parlament (Deutscher Bundestag). Cilj tega kibernetskega napada je bil informacijski sistem parlamenta, katerega delovanje je bilo nato več dni prizadeto. Ukradena je bila znatna količina podatkov, prav tako pa so bili prizadeti e-poštni računi več poslancev, tudi kanclerke Angele Merkel.	22.10.2020

▼M3

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович Костюков Datum rojstva: 21. februar 1961 Državljanstvo: rusko Spol: moški	Igor Kostyukov je trenutno vodja Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU), pred tem pa je bil prvi namestnik vodje. Ena od enot pod njegovim poveljstvom je 85. glavni center za posebne storitve (GTsSS), znan tudi kot „vojaška enota 26165“ (vzdevki v okviru panoge: „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ in „Strontium“). V tej vlogi je Igor Kostyukov odgovoren za kibernetske napade, ki jih je izvedel GTsSS, tudi tiste s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam. Vojaški obveščevalni uradniki GTsSS so sodelovali zlasti v kibernetskem napadu na nemški zvezni parlament (Deutscher Bundestag), izveden aprila in maja 2015, in v poskusu kibernetskega napada, katerega cilj je bil vdor v brezžično omrežje Organizacije za prepoved kemičnega orožja (OPCW) na Nizozemskem aprila 2018. Cilj kibernetskega napada na nemški zvezni parlament je bil informacijski sistem parlamenta, katerega delovanje je bilo nato več dni prizadeto. Ukradena je bila znatna količina podatkov, prav tako pa so bili prizadeti e-poštni računi več poslancev, tudi kanclerke Angele Merkel.	22.10.2020

▼M2

B. Pravne osebe, subjekti in organi:

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	tudi: Haitai Technology Development Co. Ltd Lokacija: Tjandžin, Kitajska	Huaying Haitai je omogočil in zagotovil finančno, tehnično ali materialno podporo za „Operation Cloud Hopper“, vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov, ki imajo pomemben učinek na tretje države.	30.7.2020

▼M2

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
			Tarča „Operation Cloud Hopper“ so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. „Operation Cloud Hopper“ je izvedel akter, v javnosti znan kot „APT10“ („Advanced Persistent Threat 10“) (tudi „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ in „Potassium“). Huaying Haitai je mogoče povezati z APT10. Poleg tega sta bila pri Huaying Haitai zaposlena Gao Qiang in Zhang Shilong, ki sta oba uvrščena na seznam v povezavi z „Operation Cloud Hopper“. Huaying Haitai je torej povezan z Gao Qiangom in Zhang Shilongom.	
2.	Chosun Expo	tudi: Chosen Expo; Korea Export Joint Venture Lokacija: DLRK	Chosun Expo je omogočil in zagotovil finančno, tehnično ali materialno podporo za vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov, ki imajo pomemben učinek na tretje države, vključno s kibernetskimi napadi, v javnosti znanimi kot „WannaCry“, in kibernetskimi napadi na poljski finančni nadzorni organ in Sony Pictures Entertainment, pa tudi kibernetsko krajo centralne banke Bangladeša in poskus kibernetske kraje vietnamske banke Tien Phong. „WannaCry“ je z izsiljevalskim virusom in onemogočanjem dostopa do podatkov povzročil motnje v informacijskih sistemih po vsem svetu. Prizadel je informacijske sisteme družb v Uniji, tudi informacijske sisteme, povezane s storitvami, potrebnimi za vzdrževanje osnovnih storitev in gospodarskih dejavnosti v državah članicah. „WannaCry“ je izvedel akter, v javnosti znan kot „APT38“ („Advanced persistent Threat 38“) ali „Lazarus Group“. Chosun Expo je mogoče povezati z APT38/Lazarus Group, tudi prek uporabniških računov, ki so bili uporabljeni za kibernetske napade.	30.7.2020

▼M2

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
3.	Glavni center za posebne tehnologije (GTsST) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU)	Naslov: Kirova ulica 22, Moskva, Ruska federacija	Glavni center za posebne tehnologije (GTsST) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU), v javnosti znan tudi kot poštni predal 74455, je odgovoren za kibernetske napade s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetske napade, ki imajo pomemben učinek na tretje države, vključno s kibernetskima napadoma junija 2017, v javnosti znanima kot „NotPetya“ ali „EternalPetya“, in kibernetskimi napadi na ukrajinsko električno omrežje pozimi leta 2015 in 2016. „NotPetya“ ali „EternalPetya“ sta z izsiljevalskim virusom in onemogočenjem dostopa do podatkov onemogočila dostop do podatkov v številnih družbah v Uniji, širši Evropi in po svetu, kar je med drugim povzročilo precejšnjo ekonomsko izgubo. Zaradi kibernetskega napada na ukrajinsko električno omrežje je pozimi prišlo do delnega izpada tega omrežja. „NotPetya“ ali „EternalPetya“ je izvedel akter, v javnosti znan kot „Sandworm“ (tudi „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ in „Telebots“), ki je odgovoren tudi za napad na ukrajinsko električno omrežje. Glavni center za posebne tehnologije pri Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije dejavno sodeluje pri kibernetskih dejavnostih, ki jih izvaja Sandworm, in ga je mogoče povezati s Sandwormom.	30.7.2020

▼M3

4.	85. glavni center za posebne storitve (GTsSS) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU)	Naslov: Komsomol’skiy Prospekt, 20, Moskva, 119146, Ruska federacija	85. glavni center za posebne storitve (GTsSS) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU), znan tudi kot „vojaška enota 26165“ (vzdevki v okviru panoge: „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ in „Strontium“), je odgovoren za kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam.	22.10.2020

▼M3

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
			Vojaški obveščevalni uradniki GTsSS so sodelovali zlasti v kibernetskem napadu na nemški zvezni parlament (Deutscher Bundestag), izveden aprila in maja 2015, in v poskusu kibernetskega napada, katerega cilj je bil vdor v brezžično omrežje Organizacije za prepoved kemičnega orožja (OPCW) na Nizozemskem aprila 2018. Cilj kibernetskega napada na nemški zvezni parlament je bil informacijski sistem parlamenta, katerega delovanje je bilo nato več dni prizadeto. Ukradena je bila znatna količina podatkov, prav tako pa so bili prizadeti e-poštni računi več poslancev, tudi kanclerke Angele Merkel.	